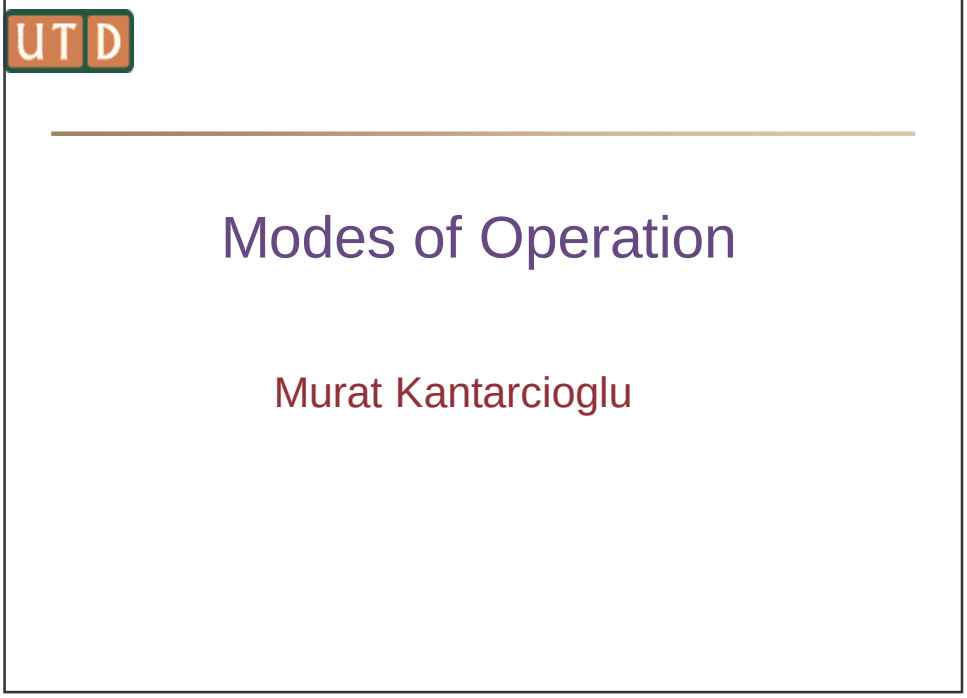
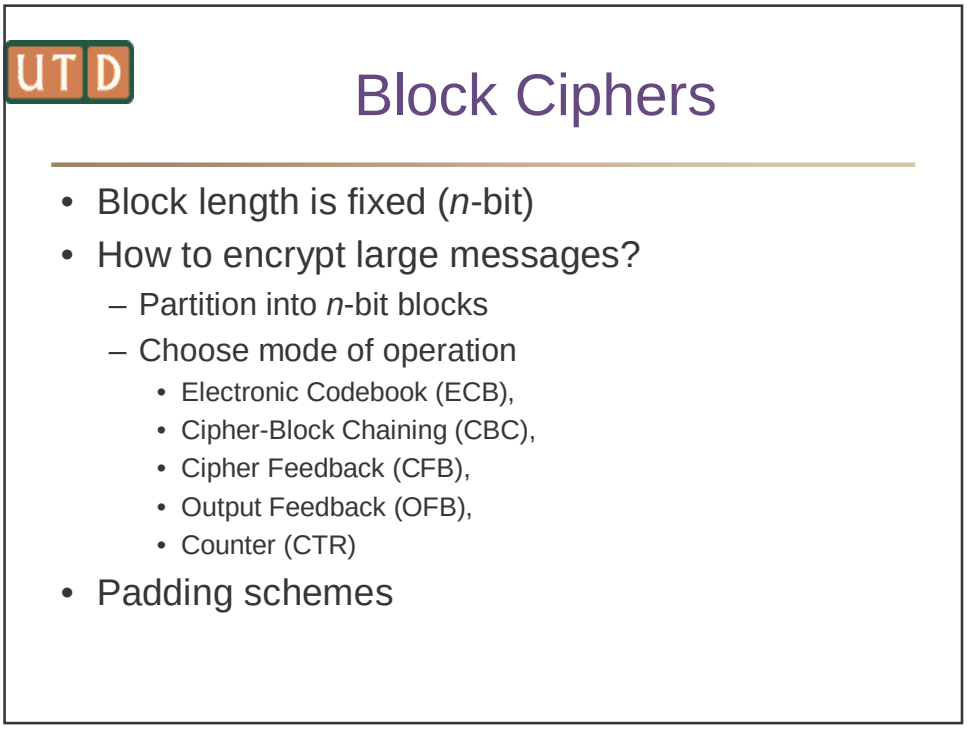

UTD
Modes of Operation
Murat Kantarcioglu


UTD
Block Ciphers
• Block length is fixed (n-bit)
• How to encrypt large messages?
– Partition into n-bit blocks
– Choose mode of operation
• Electronic Codebook (ECB),
• Cipher-Block Chaining (CBC),
• Cipher Feedback (CFB),
• Output Feedback (OFB),
• Counter (CTR)
• Padding schemes

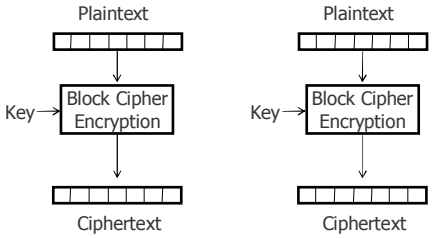
Evaluation criteria

- Identical messages
  - under which conditions ciphertext of two identical messages are the same
- Chaining dependencies
  - how adjacent plaintext blocks affect encryption of a plaintext block
- Error propagation
  - resistance to channel noise
- Efficiency
  - preprocessing
  - parallelization: random access

Notation

- Message x consists of plaintext blocks of size n
  - $x = x_1 \,||\, x_2 \,||\, \ldots \,||\, x_t$
- Ciphertext of plaintext block x_i denoted as c_i
- Chaining requires an initialization vector that first plaintext block x_1 will depend on. Initialization vector denoted as IV.
  - IV should be selected randomly for each message (x)

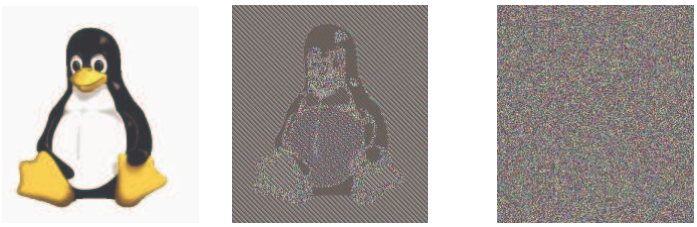
Electronic Codebook (ECB)



- Each block encrypted independently
- Identical plaintexts encrypted similarly
- No chaining, no error propagation

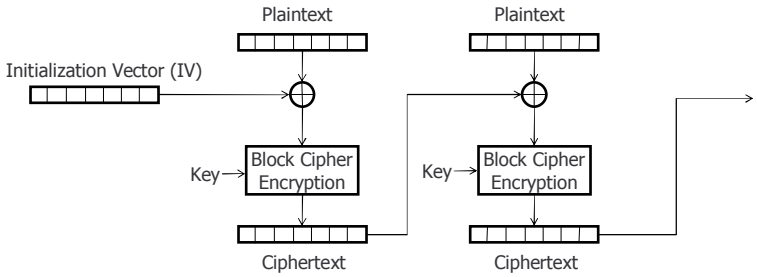
Electronic Codebook (ECB)

- Does not hide data patterns, unsuitable for long messages
  - Wiki example: pixel map using ECB



- Susceptible to replay attacks
  - Example: a wired transfer transaction can be replayed by re-sending the original message)

Cipher-Block Chaining (CBC)

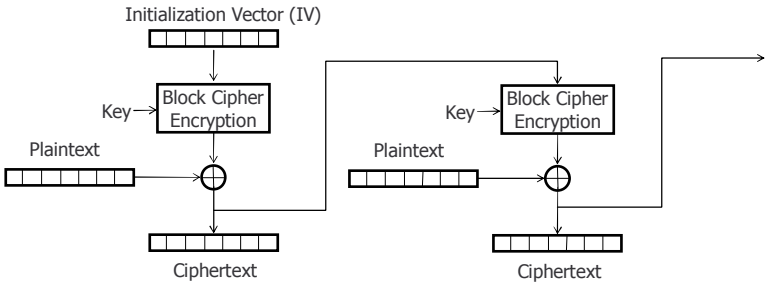


- Allows random access to ciphertext
- Decryption is parallelizable
  - Plaintext block x_j requires ciphertext blocks c_j and c_{j-1}

Cipher-Block Chaining (CBC)

- Identical messages: changing IV or the first plaintext block results in different ciphertext
- Chaining: Ciphertext block c_j depends on x_j and all preceding plaintext blocks (dependency contained in c_{j-1})
- Error propagation: Single bit error on c_j may flip the corresponding bit on x_{j+1}, but changes x_j significantly.
- IV need not be secret, but its integrity should be protected

Cipher Feedback (CFB)

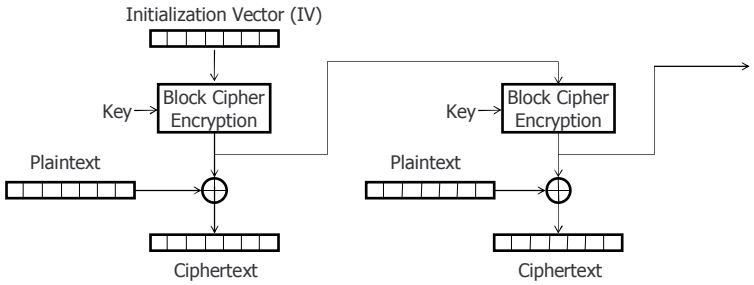


- Allows random access to ciphertext
- Decryption is parallelizable
  - Plaintext block x_j requires ciphertext blocks c_j and c_{j-1}

Cipher Feedback (CFB)

- Identical messages: as in CBC
- Chaining: Similar to CBC
- Error propagation: Single bit error on c_j may flip the corresponding bit on x_j, but changes x_{j+1} significantly.
- IV need not be secret (XORed with x_1)

Output Feedback (OFB)

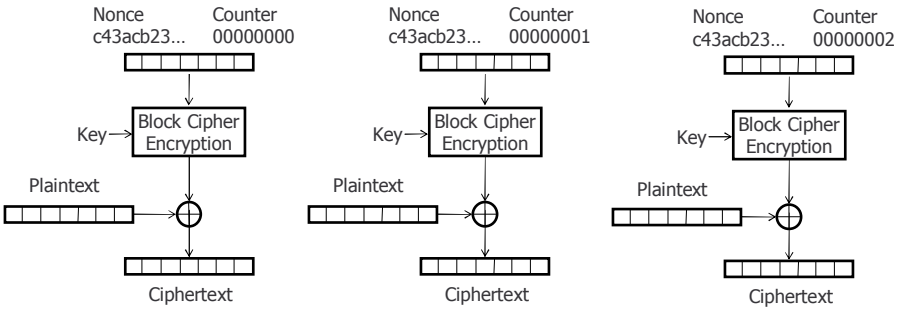


- Preprocessing possible (keep enc/decrypting previous output block)
- No random access, not parallelizable

Output Feedback (OFB)

- Identical messages: same as CBC
- No chaining dependencies
- Error propagation: Single bit error on c_j may only affect the corresponding bit of x_j
- IV need not be secret, but should be changed if a previously used key is to be used again

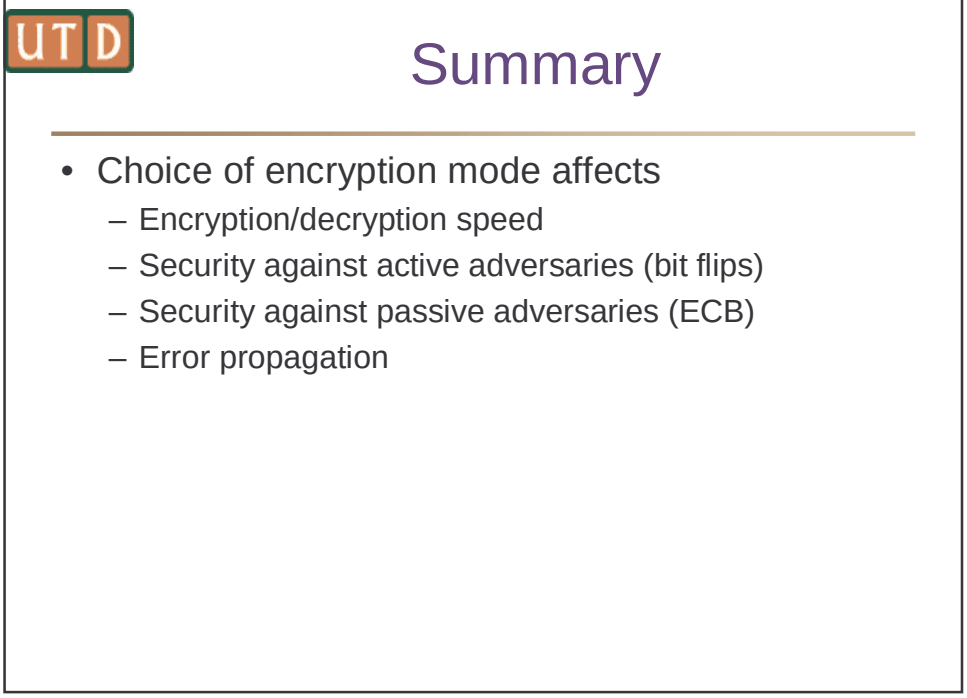
Counter (CTR)



- Preprocessing possible (inc/decrement and enc/decrypt counter)
- Allows random access

Counter (CTR)

- Both encryption & decryption are parallelizable
  - Encrypted counter is sufficient to enc/decrypt
- Identical messages: changing nonce results in different ciphertext
- No chaining dependencies
- No error propagation
- Nonce should be random, and should be changed if a previously used key is to be used again


UTD
Summary
• Choice of encryption mode affects
– Encryption/decryption speed
– Security against active adversaries (bit flips)
– Security against passive adversaries (ECB)
– Error propagation